(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2001 (27.12.2001)

PCT

(10) International Publication Number
WO 01/98875 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB01/02682

(22) International Filing Date: 18 June 2001 (18.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0014978.1 19 June 2000 (19.06.2000) GB

(71) Applicant *(for all designated States except US)*: **AMINO HOLDINGS LIMITED** [GB/GB]; Longstanton House, Woodside, Longstanton, Cambridge CB4 5BU (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GILBERT, Martyn** [GB/GB]; 41 St. Michaels, Longstanton, Cambridge CB4 5BZ (GB).

(74) Agent: **REES, Alexander, Ellison**; Urquhart-Dykes & Lord, 30 Welbeck Street, London W1G 8ER (GB).

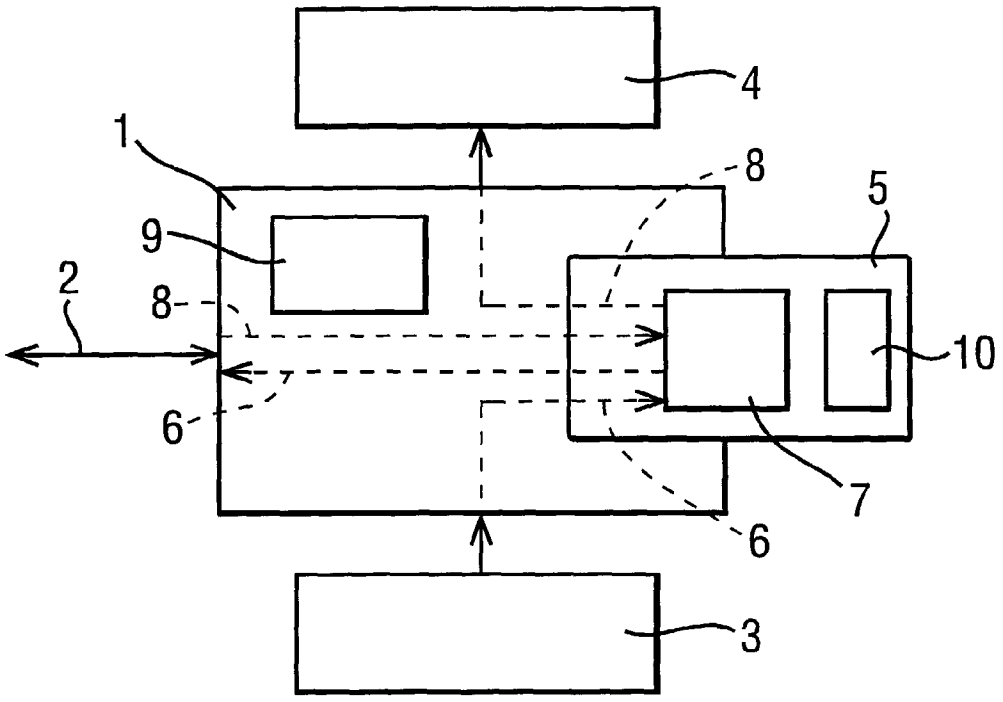
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: VALIDATION METHOD AND DEVICE



(57) Abstract: A validation method uses an interface device and a smart card. In operation, software received by the interface device together with an encrypted digest is validated by passing the encrypted digest to the smart card where it is decrypted. A digest of the software is generated and compared with the decrypted digest on the smart card and if the two digests agree, the smart cared confirms to the interface device that the software is valid.

WO 01/98875 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Validation Method and Device

This invention relates to a validation method using an interface device controlled by a smart card and to devices employing the method.

One known method of controlling access to information and services is to employ an interface device (IFD) together with a smart card.

In systems of this type the interface device controls access to information and requests for services and allows access to information or the sending of requests for services only if the presence of a valid smart card connected to the interface device is confirmed. Typically, the smart card carries one or more digital passwords and the IFD allows access to information and the issuing of requests for services only if the correct passwords are received from the smart card.

In a different approach offering a higher level of security digital passwords or encryption/decryption keys from the smart card are actually required by the IFD in order to function. For example, the issue of a password or key from the smart card may be necessary to allow the interface device to decrypt received encrypted data to be provided to a user. In such a system the IFD itself does not know what the passwords or keys from the smart card should be but the issue of the correct password is effectively confirmed by the successful decryption of the encrypted data.

Smart cards are portable devices having on-board memory and/or processing capacity. They are commonly produced in the approximate size and shape of a credit card, hence the term smart cards, but in practice can be made in any convenient shape for a particular task.

One advantage of smart card systems is that the provision of access to information and services authorised by the smart card can be separated from interface device to which the smart card is attached. For example, organisations having a computer network may allow access through terminals provided with interface devices which are physically accessible to all personnel, with the degree of access to information held on the system and authority to issue instructions through the system being controlled by smart cards issued to individuals which must be inserted into IFD's associated with the terminals. Also, hardware including the IFD to allow access to information provided by an information provider on a subscription basis may be too expensive and bulky for regular replacement of the IFD's to prevent unauthorised access by lapsed subscribers to be practical. In such systems the issue and periodic replacement of time limited smart cards to individual subscribers or the periodic issue and replacement of smart cards to all subscribers is practical because of the low cost and small size of the smart cards.

In many applications it is desirable for the software within the IFD to be alterable or updateable by the information service provider which has provided the IFD and smart card, or by someone they have authorised. Such alteration or updating of the IFD software can be carried out by uploading

software from the information service provider along the communications link.

One problem with allowing amendment or updating of the IFD software by uploading is the risk that the IFD software could be subject to unauthorised alterations, for example to alter the IFD programming to allow it be used to make cryptographic attack on the smart card or to simply delete or alter the IFD software to disable the IFD. In the first case, it is of course possible that the user themselves may attempt to reprogramme the IFD to allow cryptographic attack on the smart card.

Accordingly, it is important that any software to be loaded into the IFD is validated to ensure that it is authorised software before the software replaces existing IFD software and is used.

The present invention is intended to overcome this problem, at least in part, by providing a method and apparatus for such validation.

In a first aspect, this invention provides a validation method using an interface device and a smart card, in which software to be executed by the interface device together with encrypted data including an encrypted digest of the software is received by the interface device; a digest of the received software is calculated; the encrypted digest is loaded onto the smart card; the encrypted digest is decrypted by the smart card; and the calculated digest and the decrypted

digest are compared by the smart card in order to validate the received software.

In a second aspect, this invention provides an interface device comprising smart card interface means able to communicate with a smart card and communications means; the device is suitable for receiving software and an encrypted digest thereof by the communications means, passing the encrypted digest in encrypted form to a smart card by the interface means and executing the software only after a validation signal generated by the method of any preceding claim is received by the interface means from the smart card.

In this description references to data or software being unencrypted should be understood only as meaning that the level of encryption handled by the smart card has been decrypted or not yet applied. It is of course possible that this "unencrypted" data has had another level of encryption or encoding applied to it elsewhere.

The invention will now be described by way of example only with reference to the accompanying diagrammatic Figure, in which:
Figure 1 shows a system arranged to validate received software according to the invention.

In the present invention an interface device 1 can be connected to a system or communications network through a communications path 2.

The IFD 1 is provided with physical and electrical connections to allow a smart card 5 to be connected to and powered from the IFD 1. Such physical and electrical connections are themselves well known and need not be described in detail herein.

Preferably, a user input device 3 such as a keypad is connected to the interface device 1 in order to allow the user to make request for information to the IFD 1. Further, a display device 4 may be connected to the IFD 1 to display information provided by the IFD 1.

The key difference between the system of the present invention and known systems is that validation of software or instructions is carried out based on decryption and comparison internally within the smart card 5 itself rather than being carried out by the IFD 1 using encryption keys issued by the smart card 5.

An example of the interaction between the IFD 1 and smart card 5 is as follows. Where a request for services is made by the user, the logical data path 4 followed by the request is shown by the dashed line 6 in Figure 1.

The request, which may be a request for access to information or a request for services be provided, is generated by the user using the keyboard 3. This request is sent to the IFD 1 which sends it on to the smart card 5. The request is encrypted by an encryption/decryption element 7 of the smart card 5 and the encrypted request returned to the IFD 1. The IFD 1 then sends the encrypted request to another part of the

system or to a separate informational service provider along the communications link 2.

The reverse process is carried out when information is provided to the user, again from another part of host system or from a separate external information provider and the logical data path is shown by the dashed line 8 in Figure 1.

The encrypted information is received by the IFD 1 along the communications link 2 and the encrypted information is supplied to the smart card 5. The encryption/decryption element 7 of the smart card 5 then decrypts the received information and passes the decrypted information back to the IFD 1. The decrypted information is then supplied to the display 4 and displayed to the user.

Thus, the IFD 1 cannot display received information or send requests for information or services without a smart card 5 being present. Further, because the actual encryption and decryption is carried out by the smart card 5, it is not possible to break the security of the system by reading passwords provided by one smart card and providing these passwords to other IFD's 1.

The security or quality of the encryption employed by the system can be altered as required simply by replacing the smart card 5. The IFD 1 only has to transfer encrypted and decrypted data to and from the smart card 5 and does not carry out any encryption or decryption itself and accordingly no changes to the IFD 1 are needed when the encryption level of the smart card 5 is changed.

It should be understood that the dashed lines 6 and 8 show logical data paths only. Although the physical path followed by the data will be similar, it need not be identical. For example, there may a single set of connections carrying all data input to and from the smart card 5.

According to the invention, validation of software can be carried out as follows.

The new software purporting to be intended to be loaded into the IFD 1 is uploaded along the communications link 2 together with an encrypted digest signed or encrypted with an encryption key of an agency authorised to alter the IFD 1 software, which may be a private encryption key. The smart card 5 contains the agency's certificate which includes the agency's encryption key required to decrypt the digest which may be a public encryption key.

The digest is derived from the software. Usually the digest will be smaller than the original software, but this is not essential.

A digest of the purported software which has been uploaded is calculated from the uploaded software and compared with a decrypted version of the encrypted digest which was uploaded with the software. Only if the calculated and decrypted digests agree is the upload regarded as authorised and incorporated into the software of the IFD 1.

The term incorporated is used because the uploaded software could be intended to be added to existing software or to replace it or both.

The digest of the uploaded software could be calculated by the IFD 1 or the smart card 5 and both options will now be described.

In both methods the purported new software is uploaded along communications link 2 into the IFD 1 and is stored in an IFD memory 9.

In the first method, the IFD 1 calculates the digest of the uploaded software held in the memory 9 and sends the digest result to the smart card 5 together with the encrypted digest which was downloaded together with the software.

The smart card 5 then uses an encryption key of the software issuing agency held in a memory 10 of the smart card 5 to decrypt the encrypted digest. This may be a public encryption key. The smart card 5 then compares the calculated digest and decrypted digest and if they are the same the smart card 5 confirms to the IFD 1 that the uploaded software is valid.

If the smart card 5 confirms that the uploaded software is valid the software is incorporated into the IFD 1 operating software as appropriate. If the smart card 5 does not confirm that the uploaded software is valid, it is rejected and some alert notifying that an attempt to make authorised alterations to the IFD 1 software has occurred may be issued.

In the second method, the IFD 1 passes the purported uploaded software held in memory 9 to the smart card 5 together with the encrypted digest which accompanied the upload. The smart card 5 then calculates the digest of the uploaded software and compares this with a decryption of the encrypted digest which is decrypted using the encryption key held in the memory 10. This may be a public encryption key. If the calculated and decrypted digests agree, the smart card 5 confirms to the IFD 1 that the software is valid. The IFD 1 then responds to the confirmation or lack of confirmation as above.

In both methods security is maintained because the decrypted version of the uploaded encrypted digest and the key required to decrypt it exist within the smart card 5 only and are not transmitted to the IFD 1.

The above description is intended as a simple example only and it will be understood that many other things could be connected to the IFD 1. In particular, the user input device 3 instead of being a keyboard could itself be a computer system or device issuing requests for information services to the IFD 1 when used by user or automatically. Similarly, the display device 4 could be a conventional VDU or could be a more complex system to which data is provided.

The user input device 3 and display device 4 are not essential for the invention and may not be needed in some applications.

One example of a system according to the invention could be where the IFD was incorporated into a television set top box and in this case the requests for information would be requests for particular programs and would be generated by the television in response to user requests and the received information would be encrypted program data which would be displayed on the TV screen after decryption.

The smart card 5 has been illustrated as containing an encryption/decryption element 7 and as including a memory 10 to retain encryption keys. It should be understood that these illustrations are only intended to aid in understanding the invention and do not imply any particular physical arrangement for the smart card 5. In practice, the decryption function of the smart card 5 could be provided by a number of separate elements which may include one or more memory elements.

It is normal and convenient for the encrypted digest to be downloaded together with the software to be validated. However, this is not essential provided that the IFD is able to match the encrypted digest with the correct piece of downloaded software.

In the present application the term smart card is used for clarity because this term is commonly used to refer to devices having onboard processing capacity and/or memory. However, this should not be regarded as implying any particular physical form for the smart card 5.

It is expected that the most common and convenient method of connecting the smart card 5 to the IFD 1 to allow data and power transfer will be conductive contact. However, the invention is applicable to other forms of data and power transfer.

In order to carry out the invention, the smart card 5 only needs to be able to carry out decryption. The described embodiment uses a smart card able to carry out encryption and decryption. This is preferred in order to allow the smart card to provide other encryption based services to the IFD 1.

The term encryption key is used above to refer to keys intended both for encryption and decryption for convenience.

This description is given by way of example only and the skilled person will understand that the invention could be carried out in other ways.

CLAIMS

1. A validation method using an interface device and a smart card, in which software to be executed by the interface device together with encrypted data including an encrypted digest of the software is received by the interface device; a digest of the received software is calculated; the encrypted digest is loaded onto the smart card; the encrypted digest is decrypted by the smart card; and the calculated digest and the decrypted digest are compared by the smart card in order to validate the received software.

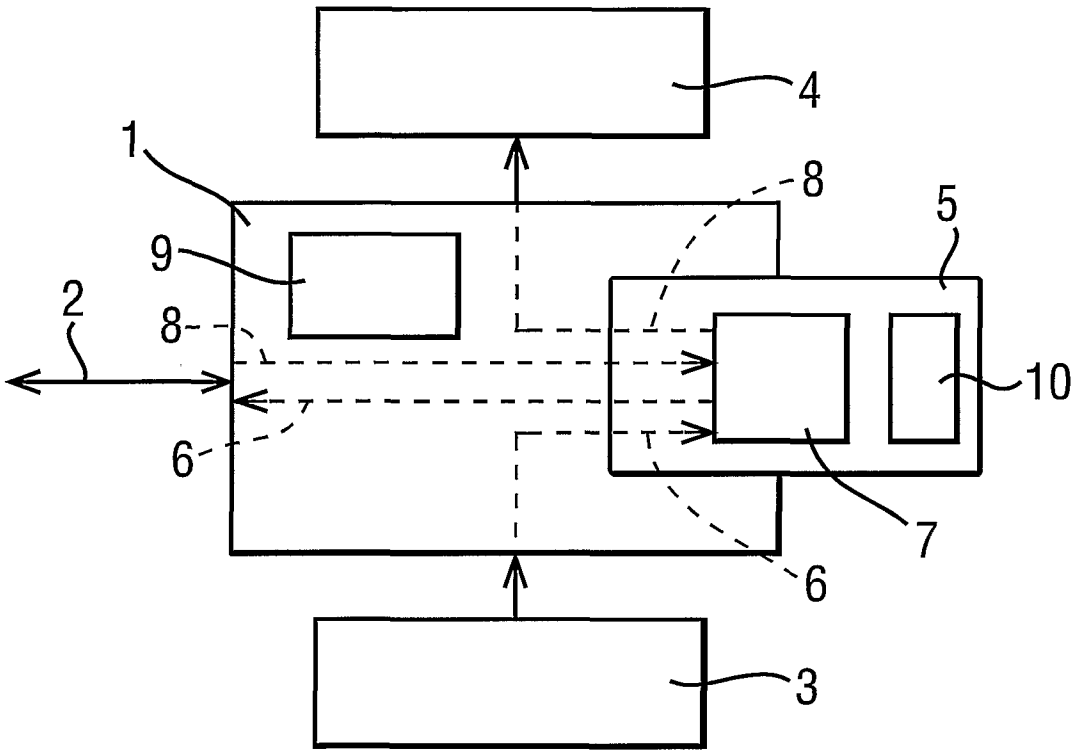
2. The method of claim 1, in which the calculated digest is calculated by the interface device and loaded onto the smart card.

3. The method of claim 1, in which the software is loaded onto the smart card and the digest is calculated on the smart card.

4. The method of any of claims 1 to 3, in which the encrypted digest is signed with a private encryption key of an authorised software supplier and the suppliers public encryption key is stored in the smart card.

5. An interface device comprising smart card interface means able to communicate with a smart card and communications means; the device is suitable for receiving software and an encrypted digest thereof by the communications means, passing the encrypted digest in encrypted form to a smart card by the interface means and executing the software only after a validation signal generated by the method of any preceding claim is received by the interface means from the smart card.

FIG.1



(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2001 (27.12.2001)

PCT

(10) International Publication Number
WO 01/098875 A3

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/GB01/02682

(22) International Filing Date: 18 June 2001 (18.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0014978.1 19 June 2000 (19.06.2000) GB

(71) Applicant *(for all designated States except US)*: **AMINO HOLDINGS LIMITED** [GB/GB]; Longstanton House, Woodside, Longstanton, Cambridge CB4 5BU (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **GILBERT, Martyn** [GB/GB]; 41 St. Michaels, Longstanton, Cambridge CB4 5BZ (GB).

(74) Agent: **REES, Alexander, Ellison**; Urquhart-Dykes & Lord, 30 Welbeck Street, London W1G 8ER (GB).

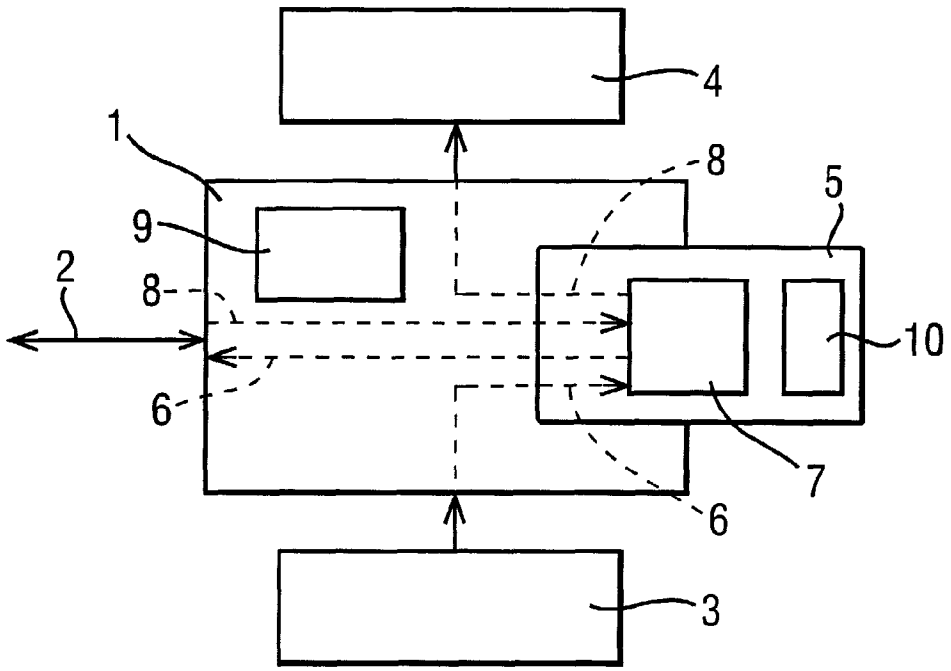
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: VALIDATION METHOD AND DEVICE



(57) Abstract: A validation method uses an interface device and a smart card. In operation, software received by the interface device together with an encrypted digest is validated by passing the encrypted digest to the smart card where it is decrypted. A digest of the software is generated and compared with the decrypted digest on the smart card and if the two digests agree, the smart cared confirms to the interface device that the software is valid.

WO 01/098875 A3

(88) Date of publication of the international search report:
23 January 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 01/02682

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 004 992 A (VISA INT SERVICE ASS) 31 May 2000 (2000-05-31) column 8, line 14 - line 29 column 9, line 30 -column 10, line 9 column 12, line 42 -column 14, line 36	1-5
X	WO 98 52163 A (MONDEX INT LTD) 19 November 1998 (1998-11-19) page 5, line 9 - line 22 page 13, line 15 -page 16, line 17 page 21, line 8 -page 22, line 18	1-5
A	WO 00 33196 A (MUIR ROBERT; LYONS MARTIN (AU); ARISTOCRAT LEISURE IND PTY LTD (AU) 8 June 2000 (2000-06-08) page 3, line 4 -page 4, line 2 page 6, line 11 - line 20	1-5

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 October 2002	04/11/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sigolo, A

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1004992 A	31-05-2000	EP 1004992 A2	31-05-2000
		AU 746459 B2	02-05-2002
		AU 6578698 A	20-10-1998
		EP 1021801 A1	26-07-2000
		US 6005942 A	21-12-1999
		US 6233683 B1	15-05-2001
		WO 9843212 A1	01-10-1998
WO 9852163 A	19-11-1998	US 6230267 B1	08-05-2001
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777098 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777298 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		DE 69807210 D1	19-09-2002
		EP 0963580 A1	15-12-1999
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0985203 A1	15-03-2000
		EP 0976114 A2	02-02-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9837526 A1	27-08-1998
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852161 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852162 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		JP 2001513231 T	28-08-2001
		JP 2001525956 T	11-12-2001
		JP 2001527674 T	25-12-2001
		JP 2001525957 T	11-12-2001
		JP 2002512715 T	23-04-2002
		JP 2001527675 T	25-12-2001
		JP 2001525958 T	11-12-2001
		US 2002050528 A1	02-05-2002
		US 6220510 B1	24-04-2001
		US 6385723 B1	07-05-2002
		US 6164549 A	26-12-2000
		US 6317832 B1	13-11-2001
		US 6328217 B1	11-12-2001
		US 2001056536 A1	27-12-2001
WO 0033196 A	08-06-2000	AU 1539300 A	19-06-2000
		WO 0033196 A1	08-06-2000